



openHPI – Sicherheit im Internet
Sicherheitsprotokolle

Prof. Dr. Christoph Meinel
Hasso-Plattner-Institut, Potsdam

Sicherheitsprotokolle (1/2)

Sicherheitsprotokolle:

- Dienen der Erreichung/Gewährleistung von **Sicherheitszielen**
- Geben Schritte vor, die die Beteiligten eines verteilten informationsverarbeitenden Prozesses befolgen müssen zur **Gewährleistung der vorgegebenen Sicherheitsanforderungen**

Beispiele:

- Authentifikationsverfahren
- Verschlüsselung, Hybride Verschlüsselung
- Digitale Signatur
- ...

Anmerkungen zur Definition

- Ziel eines Sicherheitsprotokolls ist nicht die Absicherung des Prozesses sondern die Gewährleistung der vorgegebenen Sicherheitsanforderungen
- Anders als bei Kommunikationsprotokollen darf man bei Sicherheitsprotokollen nicht davon ausgehen, dass alle Beteiligten das Protokoll vorschriftsmäßig einhalten
 - Angriffe auf Sicherheitsprotokoll zielen auf Aushebelung des Sicherheitsprotokolls oder der von diesem angewandten Verschlüsselungsverfahren zur Erlangung eines einseitigen Vorteils
- Deshalb muss sichergestellt werden, dass sich ein Sicherheitsprotokoll nicht unbemerkt missbrauchen lässt ...

Einige Anforderungen an Sicherheitsprotokolle

- **Fehlertoleranz**
 - Auch bei fehlerhaftem Verhalten/ Nutzereingaben bricht das Protokoll nicht ab, sondern bietet Lösungsmöglichkeiten
- **Verhandlungsfähigkeit**
 - Ermöglicht Einigung der Teilnehmer auf gemeinsam verwendete Verfahren und Parameter
- **Minimum Disclosure**
 - Nur allernötigste Informationen werden bekanntgegeben
- **Perfect Forward Secrecy**
 - Selbst wenn ein Verschlüsselungsschlüssel geknackt wird, darf nicht der gesamte Datenverkehr in Gefahr geraten. Es dürfen keine Rückschlüsse auf vorher verwendete Sitzungsschlüssel möglich sein

Richten sich meist an das Sicherheitsprotokoll selbst, auf die involvierten Verschlüsselungsverfahren und die dort eingesetzten Schlüssel

■ **Passive Angriffe**

- Angreifer verfolgt Ablauf der Kommunikation und versucht, Informationen über deren Inhalte und Teilnehmer zu gewinnen, z.B.
- Eavesdropping, Verkehrsflussanalyse, ...

■ **Aktive Angriffe**

- Angreifer greift in das Protokoll ein und versucht, dieses zu seinen Gunsten zu verändern, z.B.
- Spoofing, Injections, ...

■ **Replay Angriff**

- Aufzeichnen einer Nachricht und deren wiederholtes Senden

■ **Spoofing Angriffe**

- Kommunikationsaktivitäten unter falscher Identität

■ **Man-in-the-Middle Angriff**

- Unbemerkt Zwischenschalten in eine Kommunikation

■ **Hijacking Angriff**

- Kapern einer bestehenden Kommunikationsverbindung

■ **Denial-of-Service Angriff – DoS**

- Stören oder Verhindern der Kommunikation

■ ...

Zu gewährleistendes Sicherheitsziel:

Teilnehmer wollen Vertraulichkeit ihrer Nachrichten sicherstellen bei deren Transport durch einen offenen Kommunikationskanal

- Teilnehmer einigen sich zunächst auf ein gemeinsames Verschlüsselungssystem
 - Teilnehmer müssen technisch im Stande sein, die in dem Verschlüsselungssystem verwendeten Algorithmen auszuführen
 - Meist einigen sich die Teilnehmer auf das stärkste Verschlüsselungssystem, das jeder von ihnen beherrscht
- Teilnehmer verständigen sich auf einen Sitzungsschlüssel

Start der verschlüsselten Kommunikation ...

Zu gewährleistendes Sicherheitsziel:

Sicherstellung der Authentizität der Sender und der Integrität der von ihnen über ein offenes Netz versandten Nachrichten

- Teilnehmer einigen sich auf 2-Schlüssel Verschlüsselungssystem, verschaffen sich Schlüsselpaar und sorgen für eine sichere Veröffentlichung ihres öffentlichen Schlüssels
- Sender „signieren“ Nachrichten bevor sie diese versenden
 - Sender hasht Nachricht und erstellt „Signatur“ durch Verschlüsselung des Hash mit seinem privaten Schlüssel
- Empfänger kann Authentizität von Sender und Nachricht prüfen
 - Empfangene Nachricht wird gehasht und Signatur mit öffentlichem Schlüssel des Senders entschlüsselt
 - Hash und entschlüsselte Signatur werden auf Übereinstimmung geprüft ...